



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 22 octobre 2004
N° CERTA-2004-AVI-358

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans netkit-telnet

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-358>

Gestion du document

Référence	CERTA-2004-AVI-358
Titre	Vulnérabilité dans netkit-telnet et netkit-telnet-ssl
Date de la première version	22 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Debian 3.0.

3 Résumé

Une vulnérabilité présente dans les paquetages netkit-telnet et netkit-telnet-ssl peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter un code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans le traitement de la commande AYT (Are You There). Un utilisateur mal intentionné peut exploiter cette vulnérabilité pour réaliser un déni de service ou exécuter du code arbitraire avec les privilèges du service telnetd

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian dsa-556 du 18 octobre 2004 :
<http://www.debian.org/security/2004/dsa-556>
- Bulletin de sécurité Debian dsa-569 du 18 octobre 2004 :
<http://www.debian.org/security/2004/dsa-569>
- Référence CVE CAN-2004-0911 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0911>

Gestion détaillée du document

22 octobre 2004 version initiale.